JC713 U.S. PTO
10/18/99

Attorney Docket No.: CSCO-48061

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

JC599 U.S. PTO
09/420208
10/18/99

I hereby certify that this transmittal of the below described documents is being deposited with the United States Postal Service in an envelope bearing Express Mail Postage and an Express Mail label, with the below serial number, addressed to the Commissioner of Patents and Trademarks, Washington, D.C., 20231, on the below date of deposit.			
Express Mail Label No.:	EJ581806711US	Name of Person Making the Deposit:	TONY CHOU
Date of Deposit:	10/18/99	Signature of the Person Making the Deposit:	Tony Chou

Inventor(s): Shane Herman and Mahesh Walavalkar

Title: REMOTE COMPUTER SYSTEM MANAGEMENT THROUGH AN FTP INTERNET CONNECTION

The Commissioner of Patents and Trademarks
Washington, D.C. 20231
Sir:

Transmittal of a Patent Application
(Under 37 CFR §1.53)

Transmitted herewith is the above identified patent application, including:

- X Specification, claims and abstract, totaling 25 pages.
- ..... Formal drawings, totaling ..... pages.
- X Informal drawings, totaling 6 pages.
- X Declaration and Power of Attorney.
- ..... Information Disclosure statement.
- ..... Form 1449
- X Assignment(s)
- X Assignment Recordation Form (duplicate)
- ..... Preliminary Amendment

FEES DUE

The fees due for filing the specification pursuant to 37 C.F.R. § 1.16 and for recording of the Assignment, if any, are determined as follows:

CLAIMS					
	NO. OF CLAIMS		EXTRA CLAIMS	RATE	FEES
Basic Application Fee					$760.00
Total Claims	32	Minus 20=	12	X $18 =	$216.00
Independent Claims	3	Minus 3=	0	X $78=	$0.00
If multiple dependent claims are presented, add $260.00					$0.00
Add Assignment Recording Fee of $40.00 If Assignment document is enclosed					$40.00
TOTAL APPLICATION FEE DUE					$1,016.00

09420208 - 101899

PAYMENT OF FEES

The full fee due in connection with this communication is provided as follows:

1. Not enclosed

   [ ] No filing fee is to be paid at this time.

2. Enclosed

   [X] Filing fee

   [X] Recording assignment

   [ ] Petition fee for filing by other than all the inventors or person on behalf of the inventor where inventor refused to sign or cannot be reached

   [ ] For processing an application with specification in a non-English language

   [ ] Processing and retention fee

   [ ] Fee for international-type search report

   [X] The Commissioner is hereby authorized to charge any additional fees associated with this communication or credit any overpayment to Deposit Account No.: 23-0085. A duplicate copy of this authorization is enclosed.

   [X] A check in the amount of $1,016.00

   [ ] Charge any fees required or credit any overpayments associated with this filing to Deposit Account No.: 23-0085.

This application is filed pursuant to 37 C.F.R. § 1.53 in the name of the above-identified Inventor(s).

Please direct all correspondence concerning the above-identified application to the following address:

WAGNER, MURABITO & HAO LLP
Two North Market Street, Third Floor
San Jose, California 95113
(408) 938-9060

[X] This transmittal ends with this page.

Respectfully submitted,

Date: 10/18/99

By: _____
James P. Hao
Reg. No. 36,398

Express Mail Label No. EL 445 205 968 US

UNITED STATES PATENT APPLICATION

for

REMOTE COMPUTER SYSTEM MANAGEMENT THROUGH AN FTP INTERNET CONNECTION

Inventors:

Shane Herman

Mahesh Walavalkar

prepared by:

WAGNER, MURABITO & HAO LLP
Two North Market Street
Third Floor
San Jose, CA 95113
(408) 938-9060

CONFIDENTIAL

0942002.06 - 4061.95

REMOTE COMPUTER SYSTEM MANAGEMENT THROUGH AN FTP INTERNET CONNECTION

FIELD OF THE INVENTION

The present invention relates to a method for providing remote computer system management through an FTP Internet connection.

BACKGROUND OF THE INVENTION

The Internet is a general purpose, public, global computer network which allows computers hooked into the Internet to communicate and exchange digital data with other computers also on the Internet. Once a computer is coupled to the Internet, a wide variety of options become available. Some of the myriad functions possible over the Internet include sending and receiving electronic mail (e-mail) messages, logging into and participating in live discussions, playing games in real-time, viewing pictures, watching streaming video, listening to music, going shopping on-line, browsing different web sites, downloading and/or uploading files, etc.

The most popular way of participating in the Internet involves a client/server arrangement. Basically, a server computer provides a service and acts as a host to any number of client computers wishing to avail themselves of that service. For instance, a user may wish to send an e-mail message to a friend. The user first logs his or her client computer, such as a personal computer (PC)

CONFIDENTIAL

on the Internet through a standard telephone modem, cable modem, digital subscriber line (DSL), etc. The user then composes the e-mail message on the client computer which then contacts and transmits the message over the Internet to a designated e-mail server computer. Subsequently, when the recipient checks for any new e-mail messages, the recipient's client computer will contact the e-mail server. The e-mail server will then proceed to send the new e-mail message to the recipient's client computer, again over the Internet. In many cases, a server simply contains content information (e.g., web pages displaying text and/or pictures, real-time stock quotes, etc.). A huge number of clients can access this content information via the Internet.

Referring to Figure 1, a typical Internet client/server arrangement is shown. In this example, four clients 101-104 and two servers 105-106 are shown coupled to Internet 107. In general, clients 101-104 are personal computers (PC's), whereas servers 105-106 are more powerful computers with greater hardware, software, and connection resources. Any of the clients 101-104 can transmit and receive data to/from any of the servers 105-106 via Internet 107. Moreover, a single server can handle multiple client requests at the same time. Expanding upon this client/server arrangement, millions upon millions of client and server computers around the world are coupled to the vast Internet and are exchanging information, at any given time.

Presently, there are two major protocols used to establish and facilitate data transmissions between clients and servers. These protocols specify a set of technical rules by which client and server programs can communicate with one

CONFIDENTIAL

another. The first protocol is commonly referred to by its acronym, HTTP (Hypertext Transfer Protocol). HTTP is used to transfer data between servers and clients via a browser program (e.g., Navigator or Explorer) over a part of the Internet known as the World Wide Web or "the Web." HTTP enables a user to simply place a cursor on a displayed hypertext link and click on it. This automatically takes the user to the appropriate web page, to other desired information, or to another resource located on the same or different server on the Internet.

The other widely adopted protocol is known as FTP (File Transfer Protocol). FTP enables users to readily transfer files between computers over the Internet. A file is a collection of data (e.g., e-mail messages, web pages, pictures, documents, computer programs, etc.) which is stored under a given name. FTP allows a client computer to download designated files from a server and also to upload files to a server. For example, a user can design and create a web site on a local client computer, store the web pages in one or more files, and then upload these files via FTP to a web server over the Internet. These files are stored on the server and potentially anyone can now access that web page over the Internet. Thereby, FTP servers enable the distribution of software programs and other files over the Internet.

Although HTTP and FTP confer great flexibility, ease of use, and functionality to users, there are several associated drawbacks which must still be addressed. One major headache and expense involves the administration, management, and general maintenance of the servers. Ideally, the files or

CONFIDENTIAL

content stored on the servers should be secured against unauthorized users. Furthermore, whereas some users are granted permission to access the content, they should be prevented from accidentally or intentionally corrupting or otherwise altering the content stored on the servers. At the same time, legitimate owners of the content should be given permission to update or change their content as needed. It is a rather difficult task to monitor and enforce this delicate balance, especially in light of unauthorized users who attempt to crack or hack their way into secure servers. Moreover, in order to leverage the power of most server systems, a single server is often used to support an environment whereby multiple, independent file systems exist. In effect, many different users can share a single server. This necessarily entails setting up multiple accounts -- one account per user. Creating multiple accounts opens up the server system to more potential abuses by unauthorized persons.

On the one hand, server systems administrators want to grant legitimate users the ability of performing certain useful commands for administering their own virtual file systems within the server. Otherwise, the administrators themselves are faced with the overwhelming workload of having to manually and directly perform a myriad of trivial tasks for legitimate users who wish to deploy content and applications onto these servers. But on the other hand, server systems administrators would like to deny direct operating-system level access to remote clients in order to minimize security risks and to also minimize security administration overhead.

0504203.0504203 HTSB

Another related problem pertains to the fact that HTTP and FTP were designed to meet different needs. As such, these two protocols are used independently. However, with the explosion of e-commerce over the Internet, it is becoming ever more prevalent for users to utilize both protocols. For instance, rather than selling software through traditional shrink wrap packages at stores, it is becoming more cost efficient to purchase and sell software over the Internet. A customer can use a search engine to find the various sites which are offering the software product for sale. The customer can readily access these sites via HTTP to shop for the best bargain. The customer can then place an order over the Internet via HTTP. After verifying payment, the software program is then downloaded from the server to the buyer's client computer via an FTP file transfer. For the casual computer user, it may be a bit too daunting to master proficiency in both HTTP and FTP required to complete an e-commerce transaction. Furthermore, traditional businesses may have a difficult time finding the HTTP and FTP expertise necessary for transitioning into a more competitive e-commerce offering.

Thus, there is a need in the prior art for a method which removes some of the administrative burden of managing servers. There also exists a need in the prior art for improving the integrity of server systems. It would also be preferable if such a method could also somehow simplify the HTTP/FTP process inherent in e-commerce transactions. The present invention proposes a unique, novel, and elegant solution which satisfies all the above needs.

CONFIDENTIAL

SUMMARY OF THE INVENTION

The present invention pertains to a method for remote computer systems management through an FTP Internet connection. In one embodiment, a user operating on a remote client issues requests to the host server. These requests are first sent to an FTP server which enforces security measures. Upon authentication, the FTP server issues appropriate commands and then passes these commands on to the operation system of the host server through an FTP transfer. The commands perform standard features of the operation system which are not normally allowable by traditional FTP. Responses are sent back through the FTP server to the original requestor's remote client computer. Error handling, security features, and/or access controls optionally reside on top of this command-and-control request and response mechanism. Furthermore, a log file can be created to record the transactions made during each session.

In another embodiment of the present invention, a web-based management application is designed to provide an intuitive, user-friendly graphical user interface to be operated in conjunction with a web browser on the local client computer. The user submits requests through this web control panel to initiate operations to be executed on the remote operating system of the host server. These HTTP web requests are initially transmitted to a web server which processes the HTTP requests and then submits the requests to the FTP server by establishing an IP connection. The FTP server handles the requests as described in the above embodiment. Likewise, responses sent back through the FTP server

CONFIDENTIAL

are passed on to the web server and reported to the user through HTML over HTTP to the original user's web browser for display.

In yet another embodiment, by virtue of using FTP as the connection to the remote server, the present invention can be used in conjunction with remote distribution services which rely on FTP as their upload/download processes.

Dropbox - Tech Spec

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

Figure 1 shows a typical Internet client/server system.

Figure 2 shows an exemplary block diagram describing the operation of the currently preferred embodiment of the present invention.

Figure 3 shows a block diagram of an exemplary set of hardware which can be used to implement the present invention.

Figure 4 shows a diagram of a set of exemplary software blocks for practicing the present invention.

Figure 5 shows a flowchart depicting the steps of one way in which the present invention may be used.

CONFIDENTIAL

DETAILED DESCRIPTION

A method for remote computer systems management through an FTP Internet connection is described. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be obvious, however, to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to avoid obscuring the present invention.

In the currently preferred embodiment of the present invention, a user can submit requests to administer a remote computer system through a World Wide Web browser. Figure 2 shows an exemplary block diagram describing the operation of the currently preferred embodiment of the present invention. A Web-based management application is operated by a user with a Web browser 201 on the user's local computer system 202. The user can issue requests to perform certain administrative tasks on a remote computer system 205 by entering the requests through Web browser 201. By utilizing a web browser, a user can administer any remote system (e.g., a UNIX server) from any web-enabled platform or operating system, without requiring the user have direct access to, or knowledge of, the remote system or its obscure software scheme, hardware configuration, or architecture. These requests are sent over Internet 203 as HTTP to a Web server computer system 204. Web server computer system 204 processes the requests and submits corresponding commands to the remote computer system 205 through FTP over the Internet 203. These commands are

Doc#: 1603253.1

accepted and authenticated by the remote computer system 205 and then executed upon by its operating system (O/S). The remote computer operating system can be any form of operating system, including embedded operating systems (e.g., Cisco IOS) or a general purpose operating system (e.g., UNIX, NT, LINUX, Solaris, etc.). The commands initiate standard functions of the operating system which are not normally available through traditional FTP. Some exemplary commands include, but are not limited to, file and directory creation, change and edit files, remove files, Unix file mode, user and group ownership changes (for security/access permissions), and other standard system-level commands. Responses from remote computer system 205 are sent to the Web server computer system 204 as FTP over Internet 203. Web server computer system 204 forwards the responses back to the local computer system 202 as HTTP over Internet 203. The responses are displayed as HTML (Hypertext Markup Language) on Web browser 201. Error handling, security, and access controls can optionally be placed on top of this command-and-control request/response mechanism described above.

Furthermore, it should be noted that a direct connection can be established between any of the computer systems rather than an I/P (Internet Protocol) connection via the Internet. It should also be noted that the present invention is not limited to solely administering a remote computer system per se. Any type of computing, telecommunications, processing, or electronic device may be managed in this function. Some examples include concentrators, switches, routers, generators, etc. Basically, anything which runs software can be administered according to the present invention.

CONFIDENTIAL

Figure 3 shows a block diagram of an exemplary set of hardware which can be used to implement the present invention. A client computer 301 can be a personal computer (PC), portable computer, or some type of desktop computer. The client computer 301 issues HTTP requests to a Web server 302. Web server 302 processes the HTTP requests from client computer 301 and issues FTP commands to an FTP server 303. The FTP server 303 verifies and then forwards these FTP commands to the host server system 304. The operating system of host server system acts upon these commands and typically sends an FTP response back to the FTP server 303. The FTP server forwards the response to the Web server 302 which converts the FTP response into a HTTP response before forwarding it on to client computer 301. The Web server 302, FTP server 303, and Host server 304 can be one or more powerful PC's, workstations, server computers, mainframes, etc. Coupled to the host server system is a mass storage device 305 (e.g., disk array) for storing files, Web sites, documents, programs, and other types of data.

Figure 4 shows a diagram of a set of exemplary software blocks for practicing the present invention. A control panel 401 is useful to provide an easy-to-use graphical user interface (GUI) for aiding a user to enter requests to administer the remote computer system and understand any responses or acknowledgments returned from the remote computer system. The control panel can work as part of or communicate with a web browser 402 via HTML. By implementing a control panel or equivalent GUI, a user can make selections for normally command line interface systems administration calls from a web-based

CONFIDENTIAL

HP-10980408-1

GUI. Web browser 402 transmits the requests as HTML to be processed by web applications 403. The requests are then translated into FTP commands recognizable by FTP applications 404. The FTP commands affect changes to be executed upon by the operation system and/or applications 405 residing on the host server. Some of the commands may effect the creation, deletion, edit, or access of the files and data via database applications 406.

Thereby, with the present invention, certain designated on-the-box system administration privileges are extended to users and content providers operating on client computers. This grants end users the ability to perform nearly all of the administrative tasks requisite to establishing, running, and managing a file system on the remote server system. Consequently, this administrative overhead is removed from the party responsible for managing remote server system. A trusted central server can be more easily allowed to login to perform the common operating system functions. At the same time, security is not compromised because the end users are denied operating system level log-ins. By limiting the number of O/S level accounts, the security risks are correspondingly reduced. Rather than setting up an account for each user on the server, assigning a user name and password for each account, having the users Telnet into the remote system, and then granting O/S level control to the users, the present invention has only one generic entry per server. This generic entry is assigned to multiple users, and these users do not even get a password. Essentially, a generic "virtual" user takes actions on behalf of all the real users. Turning off the other IP services and ports allows greater security administration to the box or allows the remote service to be more easily deployed through

0604200.0106

firewalls, as controls to the server are carried across the same IP port as the content upload. Moreover, security can be administered from the central server system, allowing the user to potentially manage multiple remote servers from a central web-based control point. In addition, server administration managed at the central site means that remote systems do not require user account-level administration or security permissions to be established.

Figure 5 shows a flowchart depicting the steps of one way in which the present invention may be used. First, a user logs in through his or her local client computer system's control panel, step 501. Note that users can be granted access controls to the Web-based central server separately. The HTTP log-in request is sent to a web browser which acts as an entitlement hook into an FTP server. The FTP server communicates with the UNIX database manager (DBM) or LDAP to determine whether that particular user is authorized to proceed, step 502. If the user is not authorized, a message is sent back to the user for display on the client computer and authorization is denied, step 503. If the user is legitimate, the log-in is accepted. Note that in either case, there is no TELNET or O/S level log-in. Next, the privilege level granted to the user is established in step 504. Once the privilege is established, a message is sent to the user informing the user that he or she is authorized to proceed, step 505. Thereupon, the user can initiate certain commands by entering them via the control panel, step 506. These commands are accepted through the FTP server and a security check is performed on the commands, step 507. If the user does not have the requisite privilege level for that particular command, a notification is sent to the user and the command is prevented from completing, step 508. Otherwise, the FTP command is executed,

CONFIDENTIAL

step 509. It should be noted that using FTP as the connection to the remote system also means that even systems (e.g., servers) without Web-based (HTTP) or TELNET-based access can be administered using this system. Furthermore, by offering HTTP and FTP capabilities, the present invention confers extensibility to legacy systems.

Optionally, a log can be created to store all the transactions made during that session by creating a session log entry, step 510. Thereby, the system administrator has the ability to play back the log to undo certain transactions and basically rebuild the file system. This audit trail gives the system administrator a powerful management tool. Another optional step 511 entails using a single command line transaction to script the FTP server to prepare the server system for the upload of content and then proceed with the actual uploading of the content onto the remote server system, both in pre and post processing modes. The user can post commands to the web control panel which causes an HTTP web server to drive a script which, in turn, drives the FTP server. Thereby, with this embodiment, using FTP as the connection to the remote server means this can be used in conjunction with remote distribution services which rely on FTP as their upload process. Likewise, one or more scripts can be used to command the server to download files, software, data, etc., to another computer system. For example, a single script can be used to command the server to download a software program to a customer's computer system over the Internet. This same script can be used to also perform the actual FTP file download. Another example would be to use a script to update, patch, or configure software running on another system (e.g., a router, telecommunication equipment, etc). The

CONFIDENTIAL

update, patch, or configuration can be performed by someone remotely over the Internet rather than doing it on-site with shrink-wrapped, pre-packaged software. Consequently, tasks such as uploading, downloading, file posting, and directory administration can be scripted and controlled from a common central server command point. Furthermore, controls can be intermessaged with file-based upload content delivery.

Figure 6 shows an exemplary computer system upon which the present invention may be practiced. System 601 can include any computer controlled graphics systems for generating complex or three-dimensional images. Computer system 601 comprises a bus or other communication means 606 for communicating information, and a processing means 602 coupled with bus 606 for processing information. System 601 further comprises a random access memory (RAM) or other dynamic storage device 604 (referred to as main memory), coupled to bus 606 for storing information and instructions to be executed by processor 602. Main memory 604 also may be used for storing temporary variables or other intermediate information during execution of instructions by processor 602. Data storage device 605 is coupled to bus 606 for storing information and instructions. Furthermore, an I/O device 610 is used for couple the computer system 601 onto a network.

Computer system 601 can also be coupled via bus 606 to an alphanumeric input device 608, including alphanumeric and other keys, is typically coupled to bus 606 for communicating information and command selections to processor 602. Another type of user input device is cursor control

CONFIDENTIAL

609, such as a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to processor 602 and for controlling cursor movement on display 607. This input device typically has two degrees of freedom in two axes, a first axis (e.g., x) and a second axis (e.g., y), which allows the device to specify positions in a plane. It should be noted that the present invention may be implemented as a computer program running on a computer system 601. Alternatively, the present invention may be embodied as a computer program stored on a computer-readable medium, such as RAM 604 or data storage device 605 (e.g., hard disk, floppy disk, etc.).

Thus, a method for remote computer systems management through an FTP Internet connection is disclosed. The foregoing descriptions of specific embodiments of the present invention have been presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the invention to the precise forms disclosed, and obviously many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in order to best explain the principles of the invention and its practical application, to thereby enable others skilled in the art to best utilize the invention and various embodiments with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the Claims appended hereto and their equivalents.

P5420-98-US-P1

CLAIMS

What is claimed is:

1. A method for a local computer system to control a remote system over the Internet, comprising the steps of:

initiating a log-in procedure by the local computer system;

verifying whether a user is authorized to access the remote system;

accepting a command from an authorized user by the local computer system;

executing the command through a File Transfer Protocol to perform a function on the remote system.

2. The method of Claim 1 further comprising the steps of:

issuing the command through the web browser on the local computer system;

transmitting the command as HyperText Transfer Protocol over the Internet;

processing the HyperText Transfer Protocol command into a File Transfer Protocol command;

forwarding the File Transfer Protocol command to the remote system.

3. The method of Claim 2, wherein the File Transfer Protocol command includes one of the commands for file creation, directory creation,

CONFIDENTIAL

file change, file removal, Unix file mode, user ownership change, group ownership change, and security permission.

4. The method of Claim 1 further comprising the step of logging user commands for each session.

5. The method of Claim 1 further comprising the step of issuing a single script from the local computer system to command the remote system and to upload data to the remote system.

6. The method of Claim 5, wherein the data uploaded to the remote system is used to update or configure the software running on the remote system.

7. The method of Claim 1 further comprising the step of issuing a single script from the local computer system to command the remote system and to download data from the remote system.

8. The method of Claim 7, wherein the data downloaded from the remote system comprises a software program.

9. The method of Claim 1 further comprising the step of issuing command-line interface calls from a web-based graphical user interface.

0542006-040505

10. The method of Claim 1, wherein multiple users on a plurality of client computers access the remote system through a single log in.

11. The method of Claim 1, wherein the remote system is comprised of a server computer.

12. The method of Claim 1, wherein the remote system is a router.

13. The method of Claim 1 further comprising the step of managing a plurality of remote systems from a single web-based control point.

14. The method of Claim 1, further comprising the step of transmitting both commands and content through a same IP port of the remote system.

15. A server computer comprising:

an IP port which accepts FTP commands from a client computer system;

a processor coupled to the IP port which executes the FTP commands;

a first memory coupled to the processor which contains a file system;

a first memory coupled to the processor for storing an operating system, wherein a remote user issuing the FTP commands from the client computer can administer the file system.

CONFIDENTIAL

16. The server computer of Claim 15 further comprising an FTP server which accepts an HTTP command over the Internet, processes the HTTP command into a corresponding FTP command, and forwards the FTP command for execution by the processor.

17. The server computer of Claim 15, wherein the FTP command includes one of the commands for file creation, directory creation, file change, file removal, Unix file mode, user ownership change, group ownership change, and security permission.

18. The server computer of Claim 15 further comprises a third memory coupled to the processor for storing changes made during a session.

19. The server computer of Claim 15, wherein the IP port accepts a single FTP script from the client computer system which contains an instruction and which also contains content data uploaded to the server computer from the client computer system.

20. The server computer of Claim 15, wherein the IP port accepts a single FTP script from the client computer system which causes the server computer to download data from the server computer to the client computer system.

21. The server computer of Claim 20, wherein the downloaded data is comprised of a computer program.

22. The server computer of Claim 15, wherein the IP port accepts command-line interface calls from a web-based graphical user interface.

23. The server computer of Claim 15, wherein multiple users on a plurality of client computers sharing a single log-in accesses the server computer through the IP port.

24. The server computer of Claim 15, wherein a plurality of remote systems are managed from a single web-based control point running on the server computer.

25. A computer-readable medium having stored thereon instructions for implementing a remote computer systems management through an FTP Internet connection, comprising the steps of:

initiating a log-in procedure by the local computer system;

verifying whether a user is authorized to access the remote system;

accepting a command from an authorized user by the local computer system;

executing the command through a File Transfer Protocol to perform a function on the remote system.

26. The computer-readable medium of Claim 25 further storing instruction comprising the steps of:

CONFIDENTIAL

9676208.1

issuing the command through the web browser on the local computer system;

transmitting the command as HyperText Transfer Protocol over the Internet;

processing the HyperText Transfer Protocol command into a File Transfer Protocol command;

forwarding the File Transfer Protocol command to the remote system.

27. The computer-readable medium of Claim 25, wherein the File Transfer Protocol command includes one of the commands for file creation, directory creation, file change, file removal, Unix file mode, user ownership change, group ownership change, and security permission.

28. The computer-readable medium of Claim 25 further storing instruction comprising the step of logging user commands for each session.

29. The computer-readable medium of Claim 25 further storing instruction comprising the step of issuing a single script from the local computer system to command the remote system and to upload data to the remote system.

30. The computer-readable medium of Claim 25 further storing instruction comprising the step of issuing command-line interface calls from a web-based graphical user interface.

0545208.0474869

31. The computer-readable medium of Claim 25 further storing instruction comprising the step of managing a plurality of remote systems from a single web-based control point.

32. The computer-readable medium of Claim 25 further storing instruction comprising the step of transmitting both commands and content through a same IP port of the remote system.

0550206-1504

ABSTRACT OF THE DISCLOSURE

A method for remote computer systems management through an FTP Internet connection. A user operating on a remote client issues requests to the host server. These requests are first sent to an FTP server which enforces security measures. Upon authentication, the FTP server issues appropriate commands and then passes these commands on to the operation system of the host server through an FTP transfer. The commands perform standard features of the operation system which are not normally allowable by traditional FTP. Responses are sent back through the FTP server to the original requestor's remote client computer. A web-based management application may be used to provide an intuitive, user-friendly graphical user interface to be operated in conjunction with a web browser on the local client computer. The user submits requests through this web control panel to initiate operations to be executed on the remote operating system of the host server. These HTTP web requests are initially transmitted to a web server which processes the HTTP requests and then submits the requests to the FTP server by establishing an IP connection. Likewise, responses sent back through the FTP server are passed on to the web server and reported to the user through HTML over HTTP to the original user's web browser for display.

Doc#: 1601969.1

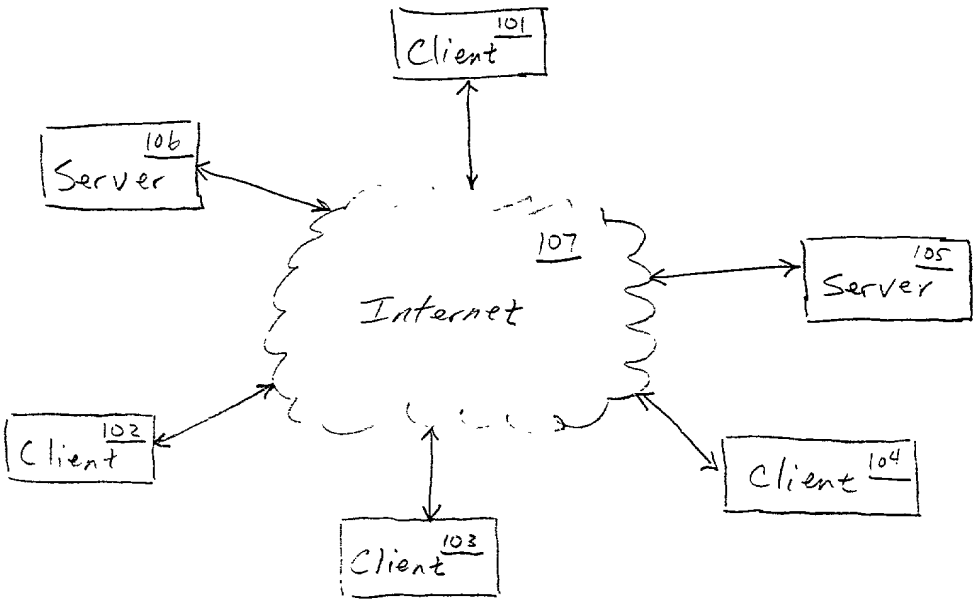


Figure 1
(Prior Art)

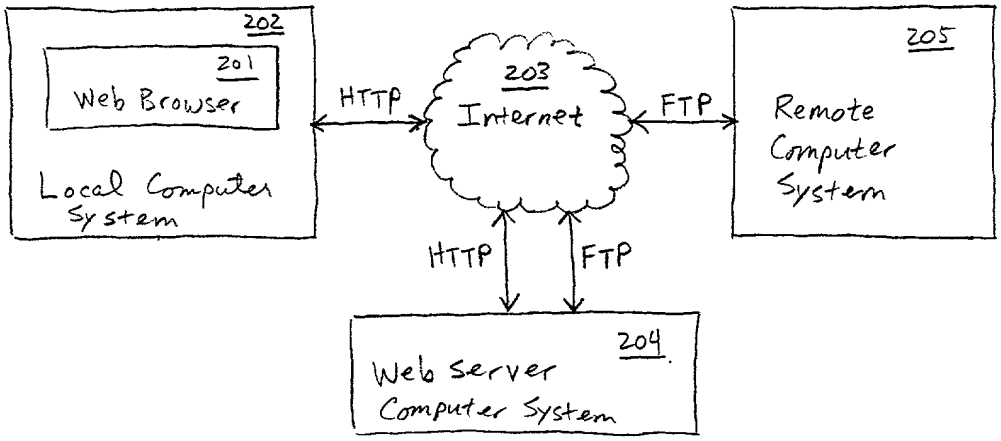

202
201
Web Browser
Local Computer System
HTTP
203
Internet
FTP
205
Remote Computer System
HTTP
FTP
204
Web server Computer System

Figure 2

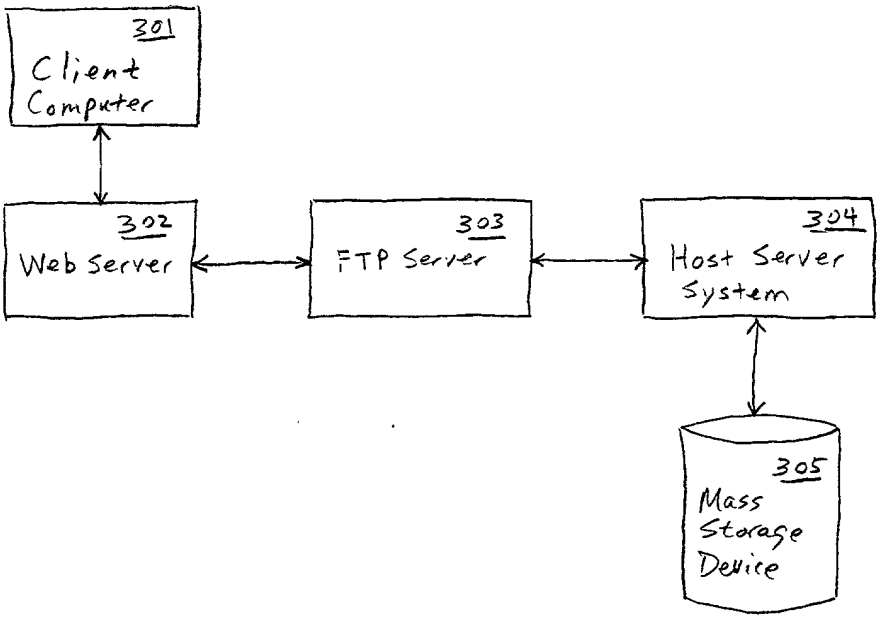


Figure 3

0540208.04169

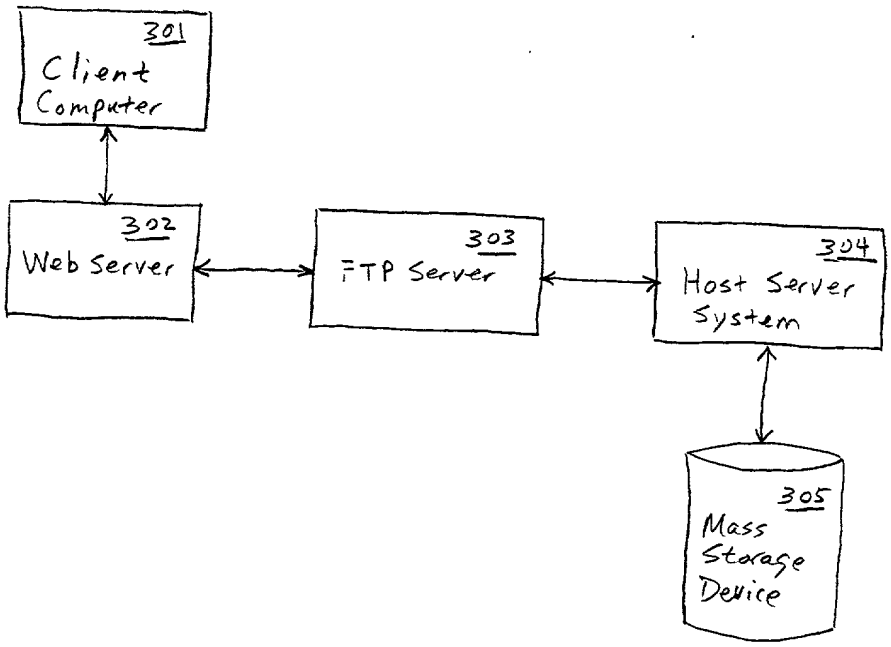


Figure 3

09420808 - 040805

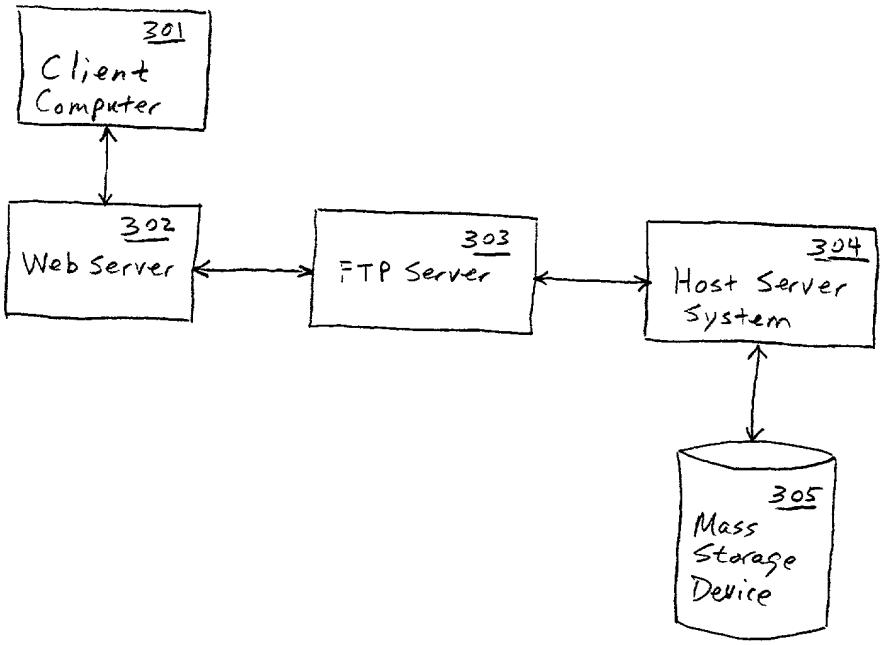

301
Client Computer
302
Web Server
303
FTP Server
304
Host Server System
305
Mass Storage Device

Figure 3

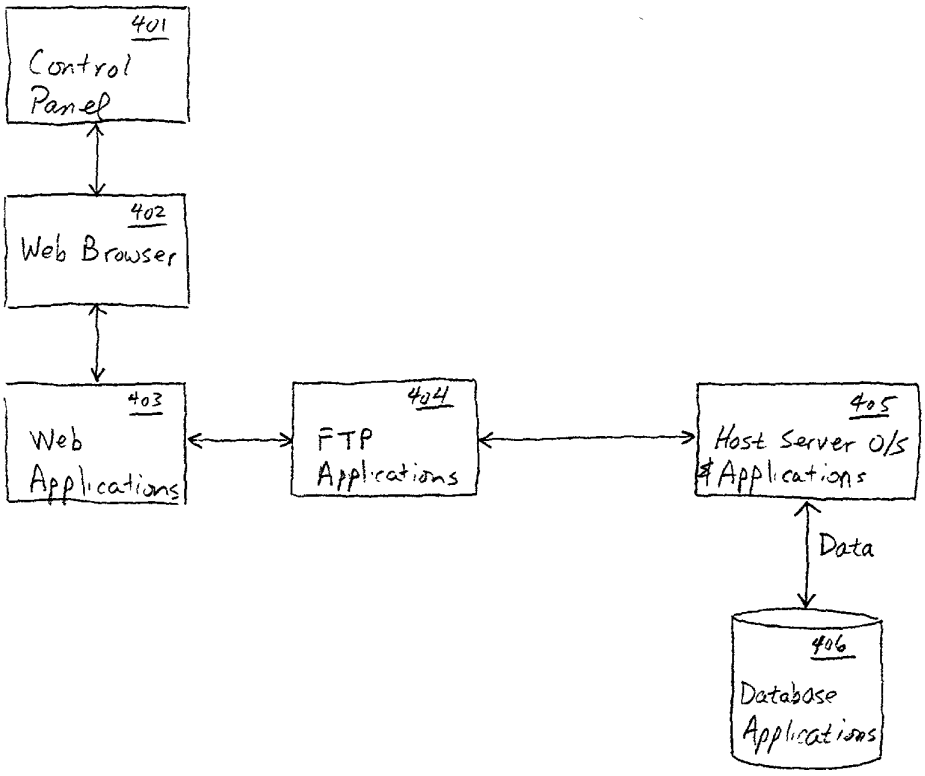

401
Control Panel
402
Web Browser
403
Web Applications
404
FTP Applications
405
Host Server O/S & Applications
Data
406
Database Applications

Figure 4

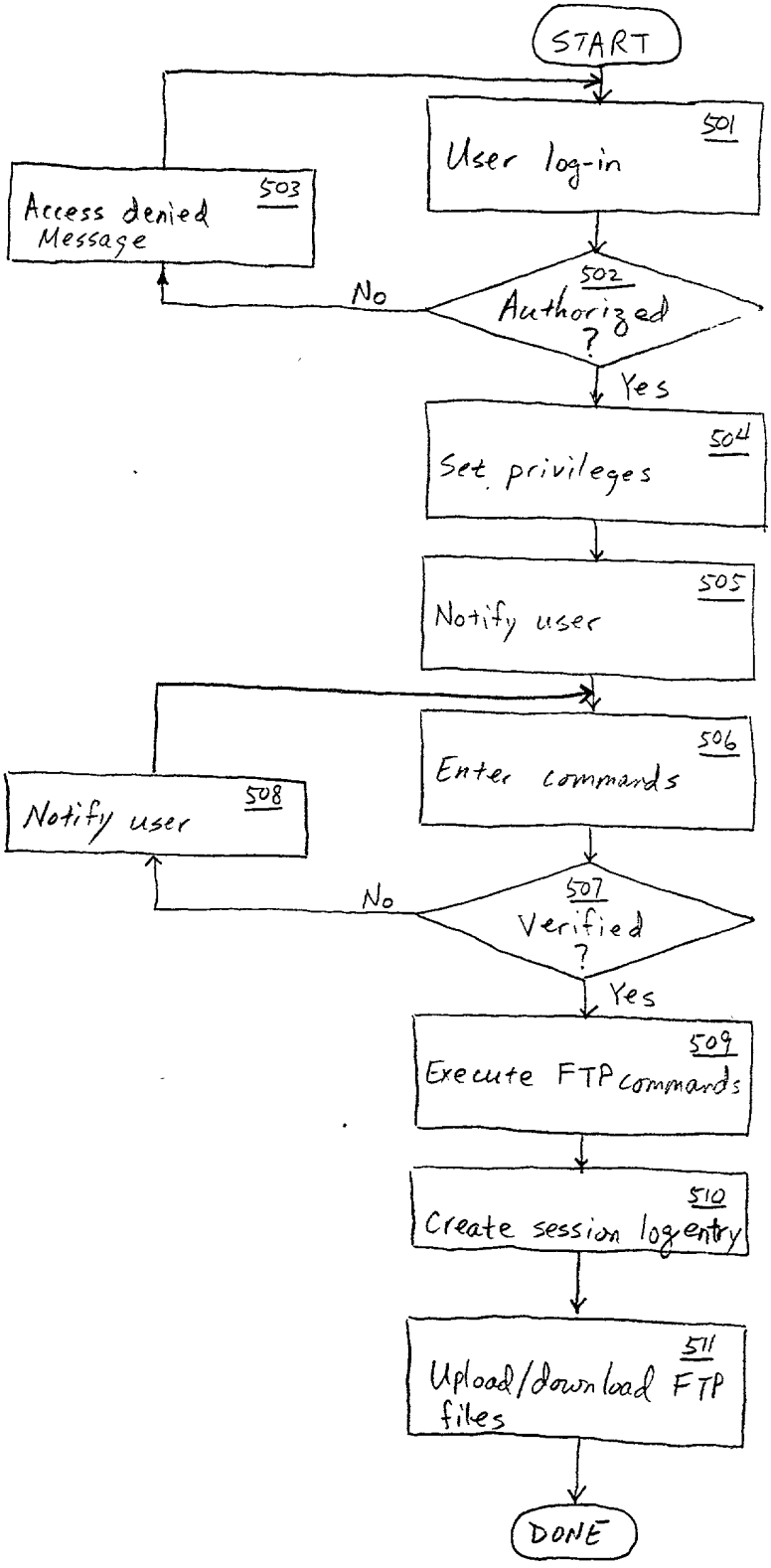

START
501
User log-in
503
Access denied Message
No
502
Authorized ?
Yes
504
Set privileges
505
Notify user
506
Enter commands
508
Notify user
No
507
Verified ?
Yes
509
Execute FTP commands
510
Create session log entry
511
Upload/download FTP files
DONE

Figure 5

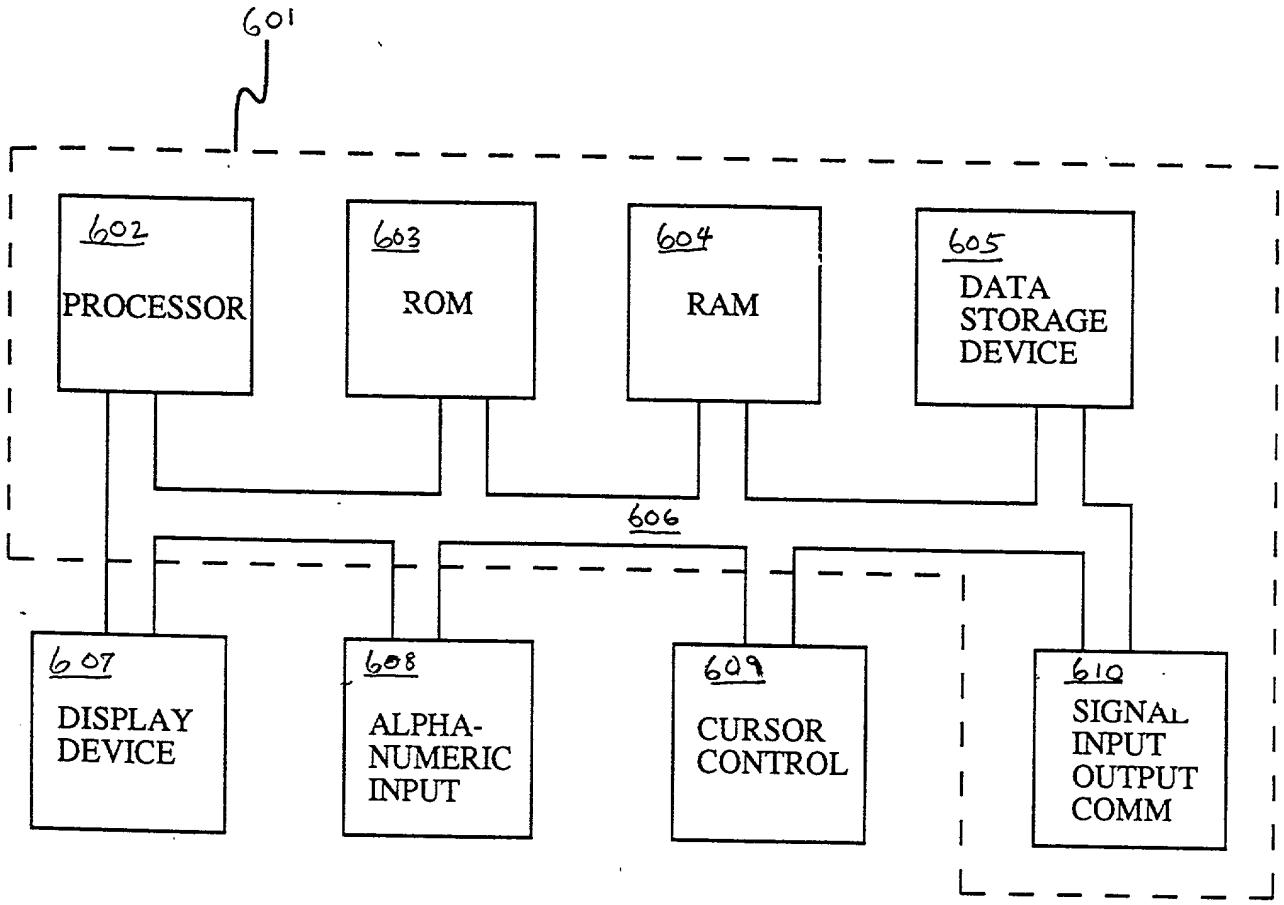

601
602
PROCESSOR
603
ROM
604
RAM
605
DATA
STORAGE
DEVICE
606
607
DISPLAY
DEVICE
608
ALPHA-
NUMERIC
INPUT
609
CURSOR
CONTROL
610
SIGNAL
INPUT
OUTPUT
COMM

FIG. 6

Declaration and Power of Attorney for a Patent Application

Declaration

As below named inventor, I hereby declare that my residence post office address, and citizenship are as stated below my name. Further, I hereby declare that I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

REMOTE COMPUTER SYSTEM MANAGEMENT THROUGH AN FTP INTERNET CONNECTION

the specification of which:

X is attached hereto, or
_____ was filed on _____ as application serial no. _____ : and
_____ was amended on _____

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above; and

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56(a).

Foreign Priority Claim

I hereby claim foreign priority benefits under Title 35, United States Code Section 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Number	Country	Date Filed	Priority Claimed	
			_____ yes	_____ no
			_____ yes	_____ no

U.S. Priority Claim

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Serial Number	Filing Date	Status (patented/pending/abandoned)

9548.0006.1

Power of Attorney

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent Trademark Office connected therewith.

James P. Hao	Registration No.: 36,398
Anthony C. Murabito	Registration No.: 35,295
John P. Wagner	Registration No.: 35,398
Glenn D. Barnes	Registration No.: 42,293
Wilfred H. Lam	Registration No.: 41,923
Patrick W. Ma	Registration No.: 44,215

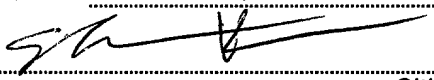
Send Correspondence to:

WAGNER, MURABITO & HAO LLP
Two North Market Street, Third Floor
San Jose, California 95113
(408) 938-9060

Signatures

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor: **Shane Herman**

Inventor's Signature  Date 10/13/09

Residence Austin, Texas (City State) Citizenship USA

P.O. Address 2001 South Mopak, #2432, Austin, Texas 78746

Full Name of Second/Joint Inventor: **Mahesh Walavalkar**

Inventor's Signature _____ Date _____

Residence Sunnyvale, California (City State) Citizenship India

P.O. Address 745 South Bernardo Ave., Apt. #370D, Sunnyvale, CA 94087

Full Name of Third/Joint Inventor: _____

Inventor's Signature _____ Date _____

Residence _____ (City State) Citizenship _____

P.O. Address _____

Google Inc. Exhibit 1006 - Page 6 of 6

Declaration and Power of Attorney for a Patent Application

Declaration

As below named inventor, I hereby declare that my residence post office address, and citizenship are as stated below my name. Further, I hereby declare that I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

REMOTE COMPUTER SYSTEM MANAGEMENT THROUGH AN FTP INTERNET CONNECTION

the specification of which:

X is attached hereto, or
_____ was filed on _____ as application serial no. _____ : and
_____ was amended on _____

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above; and

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56(a).

Foreign Priority Claim

I hereby claim foreign priority benefits under Title 35, United States Code Section 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Number	Country	Date Filed	Priority Claimed	
			____ yes	____ no
			____ yes	____ no

U.S. Priority Claim

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Serial Number	Filing Date	Status (patented/pending/abandoned)

Express Mail Label No. EL 696 704 905 US

Power of Attorney

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent Trademark Office connected therewith.

James P. Hao	Registration No.: 36,398
Anthony C. Murabito	Registration No.: 35,295
John P. Wagner	Registration No.: 35,398
Glenn D. Barnes	Registration No.: 42,293
Wilfred H. Lam	Registration No.: 41,923
Patrick W. Ma	Registration No.: 44,215

Send Correspondence to:

WAGNER, MURABITO & HAO LLP
Two North Market Street, Third Floor
San Jose, California 95113
(408) 938-9060

Signatures

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor: **Shane Herman**

Inventor's Signature _____ Date _____
Residence Austin, Texas Citizenship USA
(City State)
P.O. Address 2001 South Mopak, #2432, Austin, Texas 78746

Full Name of Second/Joint Inventor: **Mahesh Walavalkar**

Inventor's Signature Mwalavalkar Date 10/14/99
Residence Sunnyvale, California Citizenship India
(City State)
P.O. Address 745 South Bernardo Ave., Apt. #370D, Sunnyvale, CA 94087

Full Name of Third/Joint Inventor: _____

Inventor's Signature _____ Date _____
Residence _____ Citizenship _____
(City State)
P.O. Address _____

Express Mail Label No. EL474050868US